(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
18 janvier 2001 (18.01.2001)

PCT

(10) Numéro de publication internationale
WO 01/04742 A1

(51) Classification internationale des brevets⁷: G06F 7/72

(21) Numéro de la demande internationale:
PCT/FR00/01979

(22) Date de dépôt international: 7 juillet 2000 (07.07.2000)

(25) Langue de dépôt: français

(26) Langue de publication: français

(30) Données relatives à la priorité:
99/08949 9 juillet 1999 (09.07.1999) FR

(71) Déposant *(pour tous les États désignés sauf US)*: OBERTHUR CARD SYSTEMS SAS [FR/FR]; 102, boulevard Malesherbes, F-75017 Paris (FR).

(72) Inventeur; et

(75) Inventeur/Déposant *(pour US seulement)*: KNUDSEN, Erik [FR/FR]; 16, rue Alexandre Dumas, F-75011 Paris (FR).

(74) Mandataire: CABINET BONNET-THIRION; 12, avenue de la Grande Armée, Boîte postale 966, F-75829 Paris (FR).

(81) États désignés *(national)*: CA, JP, US.

(84) États désignés *(régional)*: brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Publiée:
— *Avec rapport de recherche internationale.*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(54) Title: COMPUTING METHOD FOR ELLIPTIC CURVE CRYPTOGRAPHY

(54) Titre: PROCEDE DE CALCUL POUR LA CRYPTOGRAPHIE A COURBE ELLIPTIQUE

(57) Abstract: The invention concerns fast cryptographic method between two entities exchanging data via a non-secure communication channel. The method, for example for forming a common key between two entities (A, B) each having a secret key (a, b) and using a public key (P) formed by a point of an elliptic curve (E), comprises at least a step which consists in multiplying said odd order point (P) by an integer and said phase comprises operations called additions and halving , the latter operation characterising the invention.

(57) Abrégé: Procédé de cryptographie rapide entre deux entités échangeant des informations à travers un canal de communication non sécurisé. Le procédé, par exemple pour la constitution d'une clef commune entre deux entités (A, B) possédant chacune une clef secrète (a, b) et faisant toutes deux appel à une clef publique (P) constituée par un point d'une courbe elliptique (E), comprend au moins une phase consistant à multiplier ledit point (P) d'ordre impair par un entier et cette phase comprend des opérations dites "additions" et "divisions par deux", cette dernière opération étant caractéristique de l'invention.

WO 01/04742 A1